

# Automorphism group of split Cartan modular curves

Josep González \*

## Abstract

We determine the automorphism group of the split Cartan modular curves  $X_{\text{split}}(p)$  for all primes  $p$ .

## 1 Introduction

For a prime integer  $p$ , let  $X_{\text{split}}(p)$  be the modular curve defined over  $\mathbb{Q}$  attached to the congruence subgroup of level  $p$

$$\Gamma_{\text{split}}(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : b \equiv c \equiv 0 \text{ or } a \equiv d \equiv 0 \right\}.$$

It is well-known that  $X_{\text{split}}(p)$  is isomorphic over  $\mathbb{Q}$  to the modular curve  $X_0^+(p^2) := X_0(p^2)/w_{p^2}$ , where  $w_{p^2}$  stands for the Fricke involution. The genus of this curve is positive when  $p \geq 11$  and, in this case, it is at least 2.

The automorphism group of the modular curve  $X_0(N)$  was determined, except for  $N = 63$ , by Kenku and Momose in [KM88] and was completed by Elkies in [Elk90]. Later, the automorphism group of the modular curve  $X_0^+(p) = X_0(p)/w_p$  was determined by Baker and Hasegawa in [BH03]. In this article, we focus our attention on the automorphism group of the split Cartan modular curves  $X_{\text{split}}(p)$ . Our main result is the following.

**Theorem 1.** *Assume that the genus of  $X_{\text{split}}(p)$  is positive. Then,*

$$\text{Aut}(X_{\text{split}}(p)) = \text{Aut}_{\mathbb{Q}}(X_{\text{split}}(p)) \simeq \begin{cases} \{1\} & \text{if } p > 11, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p = 11. \end{cases}$$

## 2 General facts

We recall that, for a normalized newform  $f = \sum_{n \geq 1} a_n q^n \in S_2(\Gamma_1(N))^{\text{new}}$  and a Dirichlet character  $\chi$  of conductor  $N'$ , the function

$$f_{\chi} := \sum_{n \geq 1} \chi(n) a_n q^n$$

is a cusp form in  $S_2(\Gamma_1(\text{lcm}(N, N'^2)))$  (cf. Proposition 3.1 de [AL78]). Here, as usual,  $q = e^{2\pi i z}$ . Let  $f \otimes \chi$  denote the unique normalized newform with  $q$ -expansion  $\sum_{n \geq 1} b_n q^n$  that satisfies

---

\*The author is partially supported by DGI grant MTM2012-34611.

*Keywords:* Automorphisms of modular curves, non-split Cartan subgroup.

*2010 Mathematics Subject Classification:* 14G35, 14H37.

$b_\ell = \chi(\ell)a_\ell$  for all primes  $\ell \nmid N \cdot N'$ . If  $f \otimes \chi$  is a newform of level  $M$  and  $f_\chi$  has level  $M'$ , then  $M|M'$ . Moreover, if  $M = M'$ , then  $f_\chi = f \otimes \chi$ .

We restrict ourselves to the cusp forms in  $S_2(\Gamma_0(N))$ . Let  $\text{New}_N$  denote the set of normalized newforms in  $S_2(\Gamma_0(N))^{\text{new}}$ . For  $f \in \text{New}_N$ ,  $\varepsilon(f)$  denotes the eigenvalue of  $f$  under the action of the Fricke involution  $w_N$  and set  $\text{New}_N^+ = \{f \in \text{New}_N : \varepsilon(f) = 1\}$ . For a cusp form  $f = \sum_n b_n q^n \in S_2(\Gamma_0(N))$  such that  $\mathbb{Q}(\{b_n\})$  is a number field,  $S_2(f)$  denotes the  $\mathbb{C}$ -vector space of cusp forms spanned by  $f$  and its Galois conjugates. In the particular case that  $f \in \text{New}_N$ ,  $A_f$  stands for the abelian variety attached to  $f$  by Shimura. It is well-known that  $A_f$  is a quotient of  $J_0(N) := \text{Jac}(X_0(N))$  defined over  $\mathbb{Q}$  and the pull-back of  $\Omega_{A_f/\mathbb{Q}}^1$  is the  $\mathbb{Q}$ -vector subspace of elements in  $S_2(f)dq/q$  with rational  $q$ -expansion, i.e.  $S_2(f)dq/q \cap \mathbb{Q}[[q]]$ . Moreover, the endomorphism algebra  $\text{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$  is a totally real number field.

From now on, we assume  $p \geq 11$  and  $\chi$  denotes the quadratic Dirichlet character of conductor  $p$ , i.e. the Dirichlet character attached to the quadratic number field  $K = \mathbb{Q}(\sqrt{p^*})$ , where  $p^* = (-1)^{(p-1)/2}$ .

**Lemma 1.** *The map  $f \mapsto f \otimes \chi$  is a permutation of the set  $\text{New}_{p^2} \cup \text{New}_p$ . Under this bijection, there is a unique newform  $f$ , up to Galois conjugation, such that  $f = f \otimes \chi$  when  $p \equiv 3 \pmod{4}$ .*

**Proof.** Since  $f_\chi \in S_2(\Gamma_0(p^2))$  for  $f \in \text{New}_{p^2} \cup \text{New}_p$  (cf. Theorem 3.1 of [AL78]), the level of  $f \otimes \chi$  divides  $p^2$  and, thus, the map is well defined. The injectivity follows from the fact that  $(f \otimes \chi) \otimes \chi = f$ . The condition  $f = f \otimes \chi$  amounts to saying that  $f$  has complex multiplication (CM) by the imaginary quadratic field  $K$  attached to  $\chi$ , i.e.  $p \equiv 3 \pmod{4}$ , and, moreover,  $f$  is obtained from a Hecke character  $\psi$  whose conductor is the ideal of  $K$  of norm  $p$ , which implies  $f \in \text{New}_{p^2}$ . Since  $f$  has trivial Nebentypus, the Hecke character  $\psi$  is unique up to Galois conjugation.  $\square$

**Remark 1.** *The above map does not preserve the eigenvalue of the corresponding Fricke involution, i.e. it may be that  $\varepsilon(f)$  and  $\varepsilon(f \otimes \chi)$  are different.*

**Remark 2.** *Let  $f \in \text{New}_{p^2} \cup \text{New}_p$  without CM. If  $f$  has an inner twist  $\chi' \neq 1$ , i.e.  $f \otimes \chi' = {}^\sigma f$  for some  $\sigma \in G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , then  $\chi' = \chi$  because  $\chi'$  must be a quadratic character of conductor dividing  $p^2$ . In such a case,  $\text{End}(A_f) \otimes \mathbb{Q} = \text{End}_K(A_f) \otimes \mathbb{Q}$  is a non commutative algebra. Otherwise,  $\text{End}(A_f) \otimes \mathbb{Q} = \text{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$  is a totally real number field.*

**Remark 3.** *If  $f \in \text{New}_{p^2}$  has CM, then the dimension of  $A_f$  is the class number of  $K$ ,  $A_f$  has all its endomorphisms defined over the Hilbert class field of  $K$  and  $\text{End}_K(A_f) \otimes \mathbb{Q}$  is the CM field  $\text{End}_{\mathbb{Q}}(A_f) \otimes K$  which only contains the roots of the unity  $\pm 1$  (cf. Theorem 1.2 of [GL11] and part (3) in Proposition 3.2 of [Yan04]). Moreover,  $f \in \text{New}_{p^2}^+$  if, and only if,  $p \equiv 3 \pmod{8}$  (cf. Corollary 6.3 of [MY00]).*

**Remark 4.** *For two distinct  $f_1, f_2 \in (\text{New}_{p^2} \cup \text{New}_p)/G_{\mathbb{Q}}$ , the abelian varieties  $A_{f_1}$  and  $A_{f_2}$  are nonisogenous over  $\mathbb{Q}$  and are isogenous if, and only if,  $f_1 \otimes \chi = {}^\sigma f_2$  for some  $\sigma \in G_{\mathbb{Q}}$  (see Proposition 4.2 of [GJU12]) and, in this particular case, there is an isogeny defined over  $K$ .*

The abelian variety  $J_0^+(p^2) := \text{Jac}(X_0^+(p^2))$  splits over  $\mathbb{Q}$  as the product  $(J_0(p^2)^{\text{new}})^{\langle w_{p^2} \rangle} \times J_0(p)$ . More precisely,

$$J_0^+(p^2) \stackrel{\mathbb{Q}}{\sim} \prod_{f \in (\text{New}_{p^2}^+ \cup \text{New}_p)/G_{\mathbb{Q}}} A_f. \quad (2.1)$$

Each  $f \in \text{New}_p$  provides a vector subspace of  $S_2(\Gamma_0(p^2))^{\text{old}}$  of dimension 2 generated by  $f(q)$  and  $f(q^p)$ . The normalized cusp forms  $f(q) + p\varepsilon(f)f(q^p)$  and  $f(q) - p\varepsilon(f)f(q^p)$  are eigenforms

for all Hecke operators  $T_m$  with  $p \nmid m$  and the Fricke involution  $w_{p^2}$  with eigenvalues 1 and  $-1$  respectively. The splitting of  $J_0^+(p^2)$  over  $\mathbb{Q}$  provides the following decomposition for its vector space of regular differentials

$$\Omega_{J_0^+(p^2)}^1 = \left( \bigoplus_{f \in \text{New}_{p^2}^+/G_{\mathbb{Q}}} S_2(f(q)) \frac{dq}{q} \right) \oplus \left( \bigoplus_{f \in \text{New}_p/G_{\mathbb{Q}}} S_2(f(q) + p\varepsilon(f)f(q^p)) \frac{dq}{q} \right). \quad (2.2)$$

Let  $g^+$  and  $g_0$  be the genus of the curves  $X_0^+(p^2)$  and  $X_0(p)$ , respectively. From the genus formula for these curves, one obtains the following values

$p$	$g^+$	$g_0$
$p \equiv 1 \pmod{12}$	$\frac{(p-1)(p-7)}{24}$	$\frac{p-13}{12}$
$p \equiv 5 \pmod{12}$	$\frac{(p-3)(p-5)}{24}$	$\frac{p-5}{12}$
$p \equiv 7 \pmod{12}$	$\frac{(p-1)(p-7)}{24}$	$\frac{p-7}{12}$
$p \equiv 11 \pmod{12}$	$\frac{(p-3)(p-5)}{24}$	$\frac{p+1}{12}$

### 3 Hyperelliptic case for $X_{\text{split}}(p)$

**Proposition 1.** *Assume  $p \geq 11$ . Then,  $X_{\text{split}}(p)$  is hyperelliptic if, and only if,  $p = 11$ . Moreover, one has*

$$\text{Aut}(X_{\text{split}}(11)) = \text{Aut}_{\mathbb{Q}}(X_{\text{split}}(11)) \simeq (\mathbb{Z}/2\mathbb{Z})^2.$$

**Proof.** Assume  $X_0^+(p^2)$  is hyperelliptic. By applying Lemma 3.25 of [BGGP05], we obtain  $g^+ \leq 10$ , which implies  $p \leq 19$ . We have  $g^+ = 2$  if, and only if,  $p = 11$  and, thus, the curve  $X_0^+(11^2)$  is hyperelliptic. For  $p > 11$ , one has  $g^+ > 2$  and, moreover,  $p > 13$  because  $X_0^+(13^2)$  is a plane quartic (cf. [Bar10]). Lemma 2.5 of [BGGP05] states that there is a basis  $f_1, \dots, f_{g^+}$  of  $S_2(\Gamma_0(p^2))^{\langle w_{p^2} \rangle}$  with rational  $q$ -expansions satisfying

$$f_i(q) = \begin{cases} q^i + O(q^i) & \text{if the cusp } \infty \text{ is not a Weierstrass point of } X_0^+(p^2), \\ q^{2i-1} + O(q^{2i-1}) & \text{otherwise.} \end{cases} \quad (3.1)$$

Moreover, for any such a basis, the functions on  $X_0^+(p^2)$  defined by

$$x = \frac{f_{g^+}}{f_{g^+-1}}, \quad y = \frac{qdx/dq}{f_{g^+-1}},$$

satisfy  $y^2 = P(x)$  for a unique squarefree polynomial  $P(X) \in \mathbb{Q}[X]$  which has degree  $2g^+ + 1$  or  $2g^+ + 2$  depending on whether  $\infty$  is a Weierstrass point or not. The first part of the statement follows from the fact that, for  $p = 17$  and  $p = 19$ , the vector space  $S_2(\Gamma_0(p^2))^{\langle w_{p^2} \rangle}$  does not have any bases as in (3.1).

Now, we consider  $p = 11$ . In this case,  $|\text{New}_{11^2}| = |\text{New}_{11}| = 1$ . Let  $f_1 \in \text{New}_{11^2}^+$  and let  $f_2 \in \text{New}_{11}$ . The newform  $f_1$  is the one attached to the elliptic curve  $E_1/\mathbb{Q}$  of conductor  $11^2$  with CM by  $\mathbb{Z}[(1 + \sqrt{-11})/2]$ , and  $f_2$  is the newform attached to an elliptic curve  $E_2/\mathbb{Q}$  of conductor 11 without CM. Since  $\varepsilon(f_2) = -1$ , the cusp forms  $f_1(q)$  and  $h(q) = f_2(q) - 11f_2(q^{11})$  are a basis of  $S_2(\Gamma_0(11^2))^{\langle w_{11^2} \rangle}$ . Take the following functions on  $X_0^+(11^2)$

$$x = \frac{h}{f_1} = 1 - 2q + 2q^3 - 2q^5 + O(q^5), \quad y = -2 \frac{qdx/dq}{f_1} = 4 - 8q^2 + 8q^3 + 24q^4 - 32q^5 + O(q^5).$$

Using  $q$ -expansions, we get the following equation for  $X_0^+(11^2)$ :

$$y^2 = x^6 - 7x^4 + 11x^2 + 11. \quad (3.2)$$

The maps  $(x, y) \mapsto (\pm x, \pm y)$  provide a subgroup of  $\text{Aut}_{\mathbb{Q}}(X_0^+(11^2))$  isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^2$ . Since  $\text{Aut}_{\overline{\mathbb{Q}}}(X_0^+(11^2))$  is a finite subgroup of  $\text{End}(E_1) \times \text{End}(E_2) \simeq \mathbb{Z}[(1 + \sqrt{-11})/2] \times \mathbb{Z}$ , we have that it must be a subgroup of  $(\mathbb{Z}/2\mathbb{Z})^2$ , which proves the second part of the statement.  $\square$

## 4 Preliminary lemmas

For an abelian variety  $A$  defined over a number field, we say that a number field  $L$  is the splitting field of  $A$  if it is the smallest number field where  $A$  has all its endomorphisms defined. We recall that  $K$  is the quadratic field  $\mathbb{Q}(\sqrt{p^*})$ , where  $p^* = (-1)^{(p-1)/2}p$ , and  $\chi$  is the quadratic Dirichlet character attached to  $K$ .

**Lemma 2.** *Let  $L$  be the splitting field of  $J_0^+(p^2)$ . If  $p \equiv 3 \pmod{8}$ , then  $L$  is the Hilbert class field of  $K$ . For  $p \not\equiv 3 \pmod{8}$ ,  $L = K$  if there exists  $f \in \text{New}_{p^2}^+ \cup \text{New}_p$  such that  $f \otimes \chi \in \text{New}_{p^2}^+ \cup \text{New}_p$ , otherwise  $L = \mathbb{Q}$ .*

**Proof.** On the one hand, for two distinct  $f_1, f_2 \in (\text{New}_{p^2}^+ \cup \text{New}_p)/G_{\mathbb{Q}}$  without CM,  $A_{f_1}$  and  $A_{f_2}$  are isogenous if, and only if,  $f_2$  is the Galois conjugate of  $f_1 \otimes \chi$  and, in this case, the isogeny is defined over  $K$ .

On the other hand, if  $f \in \text{New}_{p^2}^+ \cup \text{New}_p$  does not have CM, then  $f$  has at most  $\chi$  as an inner twist. In this case, the splitting field of  $A_f$  is  $K$  or  $\mathbb{Q}$  depending on whether  $\chi$  is an inner twist of  $f$  or not. If  $f$  has CM, then the splitting field of  $A_f$  is the Hilbert class field of  $K$  and  $A_f$  is unique.  $\square$

**Lemma 3.** *All automorphisms of  $X_0^+(p^2)$  are defined over  $K$ .*

**Proof.** By Lemma 2, we only have to consider the case  $p \equiv 3 \pmod{8}$  and, by Proposition 1, we can assume  $p > 11$ . Let  $g_c$  be the dimension of the abelian variety  $A_f$  with  $f \in \text{New}_{p^2}$  having complex multiplication. We know that  $g_c$  is the class number of  $K$ . Due to the fact that  $g_c = (2V - (p-1)/2)/3$ , where  $V$  is the number of quadratic residues modulo  $p$  in the interval  $[1, (p-1)/2]$ , we have  $g_c \leq (p-1)/6$ . Since  $g^+ > 1 + (p-1)/3$  for  $p > 11$  and  $p \equiv 3 \pmod{8}$ ,  $g^+ > 1 + 2g_c$ . Now, the statement is obtained by applying the same argument used in the proof of Lemma 1.4 of [KM88].  $\square$

**Lemma 4.** *The group  $\text{Aut}_{\mathbb{Q}}(X_0^+(p^2))$  is isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^s$  for some integer  $s \geq 0$ .*

**Proof.** Since  $\text{End}_{\mathbb{Q}}(J_0^+(p^2)) \otimes \mathbb{Q}$  is a product of totally real fields, any  $u \in \text{Aut}_{\mathbb{Q}}(X_0^+(p^2))$  acts as the identity or the product by  $-1$  on  $S_2(f)$  for  $f \in \text{New}_{p^2}^+$  and on  $S_2(f(q) + p\varepsilon(f)f(q^p))$  for  $f \in \text{New}_p$ . Hence,  $\text{Aut}_{\mathbb{Q}}(X_0^+(p^2))$  is isomorphic to a subgroup of  $(\mathbb{Z}/2\mathbb{Z})^r$  for  $r$  equal to  $|\text{New}_{p^2}^+/G_{\mathbb{Q}}| + |\text{New}_p/G_{\mathbb{Q}}|$ .  $\square$

**Lemma 5.** *If  $u$  is a nontrivial automorphism of  $X_0^+(p^2)$ , then  $u(\infty)$  is not a cusp.*

**Proof.** The modular curve  $X_0(p^2)$  has  $p+1$  cusps. Only the cusps  $\infty$  and  $0$  are defined over  $\mathbb{Q}$ . The remaining cusps  $1/p, \dots, (p-1)/p$  are defined over the  $p$ -th cyclotomic field  $\mathbb{Q}(\zeta_p)$ . The Galois group  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$  acts transitively on this set, and the cusp  $w_{p^2}(i/p) = (p-i)/p$  is the complex conjugate of the cusp  $i/p$  (cf. [Ogg74]). Hence, among the  $(p+1)/2$  cusps of  $X_0^+(p^2)$  the cusp  $\infty$  is the only one defined over the quadratic field  $K$ .

Let  $u$  be an automorphism of  $X_0^+(p^2)$  such that  $u(\infty)$  is a cusp. By Lemma 3,  $u(\infty)$  is defined over  $K$  and, thus,  $u(\infty) = \infty$ . Let  $\mathbb{Q}[[q]]$  be the completion of the local ring  $\mathcal{O}_{X_0^+(p^2), \infty}$  with respect to the local parameter  $q$ . If  $u(\infty)$  is the cusp  $\infty$ , then  $u^*(q) = \zeta_m q + \sum_{n>1} c_n q^n$ , where  $\zeta_m$  is a primitive  $m$ -th root of unity and, thus,  $u$  is defined over  $\mathbb{Q}(\zeta_m)$ . Since the unique roots of unity in  $K$  are  $\pm 1$ , it follows that  $u$  is defined over  $\mathbb{Q}$ .

Now, we will prove that, if  $u \in \text{Aut}_{\mathbb{Q}}(X_0^+(p^2))$  is nontrivial, then  $u(\infty) \neq \infty$ . For the hyperelliptic case  $p = 11$ , the cusp  $\infty$  has  $(1, 4)$  as  $(x, y)$  coordinates in the equation given in (3.2). Hence,  $\infty$  is not a fixed point for any of the three nontrivial involutions of  $X_0^+(11^2)$ . Let  $p > 11$ . Since  $X_0^+(p^2)$  is nonhyperelliptic and, by Lemma 5,  $u$  is an involution, we can exclude the case where all eigenvalues of  $u$  acting on  $\Omega_{J_0^+(p^2)}^1$  are equal to  $-1$  and, thus,  $u$  must have eigenvalues  $1$  and  $-1$  acting on this vector space. The vector space of cusp forms  $\Omega_{J_0^+(p^2)}^1 q/dq$  has a basis of normalized eigenforms (see (2.2)). Since  $u$  is defined over  $\mathbb{Q}$ ,  $u$  commutes with the Hecke operators and, thus, there are two normalized eigenforms such that their corresponding regular differentials  $\omega_1 = (1 + \sum_{n>1} a_n q^n) dq$  and  $\omega_2 = (1 + \sum_{n>1} b_n q^n) dq$  satisfy  $u^*(\omega_1) = \omega_1$  and  $u^*(\omega_2) = -\omega_2$ . Hence,  $u$  sends  $\omega_1 + \omega_2$ , which does vanish at  $\infty$ , to  $\omega_1 - \omega_2$ , which vanishes at  $\infty$ .  $\square$

Let  $\nu \in \text{Gal}(K/\mathbb{Q})$  be the conjugation corresponding to the Frobenius element of the prime 2. The following lemma is an adapted version of Lemma 3.3 of [BH03] to our context, restricted to the prime 2.

**Lemma 6.** *Assume that  $u \in \text{Aut}(X_0^+(p^2))$  is nontrivial. For any noncuspidal point  $S \in X_0^+(p^2)(\mathbb{C})$ , the divisor*

$$D_S := (uT_2 - T_2u^\nu)(\infty - S),$$

*where  $T_2$  denotes the Hecke operator viewed as a correspondence of the curve  $X_0^+(p^2)$ , is nonzero but linearly equivalent to zero. In particular, the  $K$ -gonality of  $X_0^+(p^2)$  is at most 6 and  $u$  has at most 12 fixed points.*

**Proof.** Following the arguments used in Lemma 2.6 of [KM88], one has  $uT_2 = T_2u^\nu$  and, thus,  $D_S$  is a principal divisor. Set  $Q = u(\infty)$  and let  $P \in X_0(p^2)(\overline{\mathbb{Q}})$  be such that  $\pi^+(P) = Q$  where  $\pi^+ : X_0(p^2) \rightarrow X_0^+(p^2)$  is the natural projection. Since  $Q$  is not a cusp, there is an elliptic curve  $E$  defined over  $\overline{\mathbb{Q}}$  and a  $p^2$ -cyclic subgroup  $C$  of  $E(\overline{\mathbb{Q}})$  such that  $P = (E, C)$ . The other preimage of  $Q$  under  $\pi^+$  is the point  $w_{p^2}(P) = (E/C, E[p^2]/C)$ .

If  $D_S$  is a zero divisor, then  $uT_2(\infty)$  must be equal to  $T_2u^\nu(\infty)$  because  $T_2(\infty) = 3\infty$  and  $\infty$  is not in the support of  $T_2(S)$ . To prove that  $D_S$  is a nonzero divisor, we only need to prove that the condition  $3(Q) = T_2(Q^\nu)$  cannot occur.

Let  $C_i$ ,  $1 \leq i \leq 3$ , be the three 2-cyclic subgroups of  $E^\nu[2]$ . Since

$$T_2(Q^\nu) = \sum_{i=1}^3 \pi^+((E^\nu/C_i, C)),$$

the condition  $3(Q) = T_2(Q^\nu)$  implies that each elliptic curve  $E^\nu/C_i$  is isomorphic to  $E$  or  $E/C$ . So, at least two quotients  $E^\nu/C_i$  are isomorphic and, thus,  $E^\nu$  must be an elliptic curve with CM by the order  $\mathcal{O}$ , where  $\mathcal{O}$  is the ring of integers  $\mathbb{Z}[\sqrt{-1}]$ ,  $\mathbb{Z}[(1 + \sqrt{-3})/2]$ ,  $\mathbb{Z}[(1 + \sqrt{-7})/2]$  or  $\mathbb{Z}[(1 + \sqrt{-15})/2]$ . For the first three cases,  $E^\nu$  is defined over  $\mathbb{Q}$  and, in the last case, it is defined over  $\mathbb{Q}(\sqrt{5})$ . In any case,  $E^\nu = E$ . We prove that, in all these cases, there is a subgroup  $C_i$  such that  $E/C_i$  has CM by the order  $2\mathcal{O}$  and this order contains an element of norm  $2p^2$ , which is not possible.

In the first case, all elliptic curves  $E/C_i$  are isomorphic and have CM by the order  $2\mathcal{O}$ . Hence,  $E/C_i$  must be isomorphic to  $E/C$  and, thus, there is a  $2p^2$ -cyclic isogeny from  $E/C_i$  to itself. This leads to the existence of an element in the order  $2\mathcal{O}$  of norm  $2p^2$ .

In the second and third cases,  $E$  is isomorphic to two curves  $E/C_1$  and  $E/C_2$ , while  $E/C_3$  is the elliptic curve with CM by  $2\mathcal{O}$ . Hence,  $E/C_3 \simeq E/C$  and, thus, we can derive the existence of an element in  $2\mathcal{O}$  of norm  $2p^2$ .

In the last case,  $E$  is defined over  $\mathbb{Q}(\sqrt{5})$ . Two quotients  $E/C_1$  and  $E/C_2$  are isomorphic to the nontrivial Galois conjugated curve of  $E$ , and the curve  $E/C_3$  has CM by the order  $2\mathcal{O}$ . Hence,  $E/C_3$  is not isomorphic to  $E$  and should be isomorphic to  $E/C$ . Again, we obtain the existence of an element in  $2\mathcal{O}$  of norm  $2p^2$ .

By taking  $S = u(\infty)$ ,  $D_S$  is defined over  $K$  and, thus, the  $K$ -gonality is at most 6. Finally, since  $u^*(D_S) \neq D_S$  for some noncuspidal point  $S \in X_0^+(p^2)(\mathbb{C})$ , any nontrivial automorphism of  $X_0^+(p^2)$  has at most 12 fixed points (cf. Lemma 3.5 of [BH03]).  $\square$

**Lemma 7.** *If  $X_0^+(p^2)$  has a nontrivial automorphism and  $p > 11$ , then  $p \in \{17, 19, 23, 29, 31\}$ .*

**Proof.** By applying Lemma 3.25 of [BGGP05] for the prime 2, we obtain that

$$g^+ < X_0^+(p^2)(\mathbb{F}_4) + 1.$$

By Lemma 6, the  $\mathbb{F}_4$ -gonality of  $X_0^+(p) \otimes \mathbb{F}_4$  is  $\leq 6$  and, thus,  $X_0^+(p)(\mathbb{F}_4) \leq 30$ . Hence,  $g^+ \leq 30$ , which implies  $p \leq 31$ . The algebra  $\text{End}(J_0^+(13^2)) \otimes \mathbb{Q}$  is a totally real number field and, thus, it only contains the roots of unity  $\pm 1$ . Since  $X_0^+(13^2)$  is nonhyperelliptic,  $\text{Aut}(X_0^+(13^2))$  is trivial and we can discard the case  $p = 13$ .  $\square$

**Lemma 8.** *Every nontrivial automorphism of  $X_0^+(p^2)$  has even order.*

**Proof.** Assume that there is a nontrivial automorphism  $u$  of  $X_0^+(p^2)$  whose order  $m$  is odd. Let  $X_u$  be the quotient curve  $X_0^+(p^2)/u$  and denote by  $g_u$  its genus. Next, we find a positive lower bound  $t$  for  $g_u$ .

The endomorphism algebra  $\text{End}_K(J_0^+(p^2)) \otimes \mathbb{Q}$  is the product of some noncommutative algebras and some number fields  $E_f = \text{End}_K(A_f) \otimes \mathbb{Q}$  attached to the newforms  $f$  lying in a certain subset  $\mathcal{S}$  of  $(\text{New}_{p^2}^+ \cup \text{New}_p)/G_{\mathbb{Q}}$ . The set  $\mathcal{S}$  is formed by newforms  $f$  without CM such that  $f \otimes \chi \notin \text{New}_{p^2}^+ \cup \text{New}_p$  ( $E_f = \text{End}_{\mathbb{Q}}(A_f)$  is a totally real number field) and by a newform  $f$  with CM by  $K$  if  $p \equiv 3 \pmod{8}$  ( $E_f = \text{End}_{\mathbb{Q}}(A_f) \otimes K$  is a CM field). For  $f \in \mathcal{S}$ , the unique root of unities contained in  $E_f$  are  $\pm 1$ . Since  $m$  is odd, the automorphism  $u$  must act on each  $E_f$  as the identity and, thus, we have

$$t := \sum_{f \in \mathcal{S}} \dim A_f \leq g_u.$$

An easy computation provides the following values for  $t$ :

$p$	17	19	23	29	31
$g^+$	7	9	15	26	30
$t$	5	5	7	15	12

Applying Riemann-Hurwitz formula,

$$m \leq \frac{g^+ - 1}{g_u - 1} \leq \frac{g^+ - 1}{t - 1} < 3,$$

which yields a contradiction.  $\square$

## 5 Proof of Theorem 1

Assume that, for  $p \in \{17, 19, 23, 29, 31\}$ , there is a nontrivial automorphism  $u \in \text{Aut}_K(X_0^+(p^2))$ . By Lemma 8, we can suppose that  $u$  is an involution. Let  $g_u$  be the genus of the quotient curve  $X_0^+(p^2)/u$ . We know that  $u$  has at most 12 fixed points. By Riemann-Hurwitz formula, we get that the number of fixed points by  $u$  must be even, say  $2r$ , and, moreover,

$$g_u = \frac{g^+ + 1 - r}{2}, \quad 0 \leq r \leq 6.$$

If  $g^+$  is even, then  $u$  can have 2, 6 or 10 ramification points, while for the case  $g^+$  odd,  $u$  can have 0, 4, 8 or 12 such points.

For a prime  $\ell \neq p$ , the curve  $X = X_0^+(p^2)$  has good reduction at  $\ell$ . Let  $\tilde{X}$  be the reduction of  $X$  modulo  $\ell$ . We write

$$N_\ell(n) := 1 + \ell^n - \sum_{i=1}^{2g^+} \alpha_i^n,$$

where  $\alpha_1, \dots, \alpha_{2g^+}$  are the roots of polynomial

$$\prod_{f \in \text{New}_{p^2}^+ \cup \text{New}_p} (x^2 - a_\ell(f)x + \ell)$$

and  $a_\ell(f)$  is the  $\ell$ -th Fourier coefficient of  $f$ . By Eichler-Shimura congruence,  $N_\ell(n) = |\tilde{X}(\mathbb{F}_{\ell^n})|$ .

Let  $\mathfrak{l}$  be a prime of  $K$  over  $\ell$  with residue degree  $s$ . The reduction of  $X \otimes K$  modulo  $\mathfrak{l}$  is  $\tilde{X} \otimes \mathbb{F}_{\ell^s}$  which has an involution, say  $\tilde{u}$ , with at most  $2r$  fixed points. The automorphism  $\tilde{u}$  acts on the set  $\tilde{X}(\mathbb{F}_{\ell^s n})$  as a permutation. If  $Q \in \cup_{i=1}^n \tilde{X}(\mathbb{F}_{\ell^s i})$ , then the set  $\mathcal{S}_Q = \{\tilde{u}^i(Q) : 1 \leq i \leq 2\}$  is contained in  $\cup_{i=1}^n \tilde{X}(\mathbb{F}_{\ell^s i})$  and its cardinality is equal to 1 or 2 according to  $Q$  is a fixed point of  $\tilde{u}$  or not. Hence, almost all integers  $R_\ell(n) := |\cup_{i=1}^n \tilde{X}(\mathbb{F}_{\ell^s i})|$ ,  $n \geq 1$ , are equivalent to the number of fixed points of  $\tilde{u} \bmod 2$  and, moreover, the sequence  $\{R_\ell(n)\}_{n \geq 1}$  can only contain at most  $2r$  or  $2r - 1$  changes of parity depending on whether  $N_\ell(s)$  is even or odd. In other words, the sequence of integers  $\{P_\ell(n)\}_{n \geq 1}$  defined by

$$0 \leq P_\ell(n) \leq 1 \quad \text{and} \quad P_\ell(n) = R_\ell(n+1) - R_\ell(n) \pmod{2},$$

can only contain at most  $2r$  or  $2r - 1$  ones according to  $N_\ell(s)$  being even or odd.

Note that the integer  $R_\ell(n+1) - R_\ell(n)$  can be obtained from the sequence  $\{N_\ell(sn)\}$  by using

$$\tilde{X}(\mathbb{F}_{\ell^s d_1}) \cap \tilde{X}(\mathbb{F}_{\ell^s d_2}) = \tilde{X}(\mathbb{F}_{\ell^s \gcd(d_1, d_2)}), \quad \text{and if } d_1 | d_2 \text{ then } \tilde{X}(\mathbb{F}_{\ell^s d_1}) \cup \tilde{X}(\mathbb{F}_{\ell^s d_2}) = \tilde{X}(\mathbb{F}_{\ell^s d_2}).$$

More precisely, if  $\{p_1, \dots, p_r\}$  is the set of primes dividing  $n+1$  and we put  $d_i = (n+1)/p_i$  for  $1 \leq i \leq r$ , then

$$R_\ell(n+1) - R_\ell(n) = P_\ell(s(n+1)) - \sum_{j=1}^r (-1)^{r-1} \sum_{1 \leq i_1 < \dots < i_j \leq r} P_\ell(s \gcd(d_{i_1}, \dots, d_{i_j})).$$

For the five possibilities for  $p$ , we have:

$p = 31$ :  $g^+ = 30$ ,  $2r \leq 10$  and  $\ell = 2$  splits in  $K = \mathbb{Q}(\sqrt{-31})$ . One has

$$N_2(1) = 9, \quad \sum_{n \leq 36} P_2(n) = 10.$$

$p = 29$ :  $g^+ = 26$ ,  $2r \leq 10$  and  $\ell = 2$  is inert in  $K = \mathbb{Q}(\sqrt{29})$ . One has

$$N_2(2) = 42, \quad \sum_{n \leq 42} P_2(n) = 11.$$

$p = 23$ :  $g^+ = 15$ ,  $2r \leq 12$  and  $\ell = 2$  splits in  $K = \mathbb{Q}(\sqrt{-23})$ . One has

$$N_2(1) = 8, \quad \sum_{n \leq 38} P_2(n) = 13.$$

$p = 19$ :  $g^+ = 9$ ,  $2r \leq 12$  and  $\ell = 2$  is inert in  $K = \mathbb{Q}(\sqrt{-19})$ . One has

$$N_2(2) = 22, \quad \sum_{n \leq 46} P_2(n) = 13.$$

$p = 17$ :  $g^+ = 7$ ,  $2r \leq 12$  and  $\ell = 2$  splits in  $K = \mathbb{Q}(\sqrt{17})$ . One has

$$N_2(1) = 6, \quad \sum_{n \leq 46} P_2(n) = 13.$$

So, we can discard the five cases considered and the statement is proved.

## References

- [AL78] A. O. L. Atkin and Wen Ch'ing Winnie Li. Twists of newforms and pseudo-eigenvalues of  $W$ -operators. *Invent. Math.*, 48(3):221–243, 1978.
- [Bar10] B. Baran. Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. *J. Number Theory*, 130(12):2753–2772, 2010.
- [BGGP05] M. Baker, E. González-Jiménez, J. González, and B. Poonen. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.*, 127(6):1325–1387, 2005.
- [BH03] M. Baker and Y. Hasegawa. Automorphisms of  $X_0^*(p)$ . *J. Number Theory*, 100(1):72–87, 2003.
- [Elk90] N. D. Elkies. The automorphism group of the modular curve  $X_0(63)$ . *Compositio Math.*, 74(2):203–208, 1990.
- [GJU12] J. González and J. Jiménez-Urroz. The Sato-Tate distribution and the values of Fourier coefficients of modular newforms. *Experiment. Math.*, 21(1):84–102, 2012.
- [GL11] J. González and J-C. Lario. Modular elliptic directions with complex multiplication (with an application to Gross's elliptic curves). *Comment. Math. Helv.*, 86(2):317–351, 2011.
- [KM88] M. A. Kenku and Fumiyuki Momose. Automorphism groups of the modular curves  $X_0(N)$ . *Compositio Math.*, 65(1):51–80, 1988.
- [MY00] S. D. Miller and T. Yang. Non-vanishing of the central derivative of canonical Hecke  $L$ -functions. *Math. Res. Lett.*, 7(2-3):263–277, 2000.



- [Ogg74] A. P. Ogg. Hyperelliptic modular curves. *Bull. Soc. Math. France*, 102:449–462, 1974.
- [Yan04] T. Yang. On CM abelian varieties over imaginary quadratic fields. *Math. Ann.*, 329(1):87–117, 2004.

Josep González  
josepg@ma4.upc.edu  
Departament de Matemàtica Aplicada 4  
Universitat Politècnica de Catalunya  
EPSEVG, Avinguda Víctor Balaguer 1  
08800 Vilanova i la Geltrú, Spain